OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

This document is designed to help federally regulated financial institutions (the FRFI) supervised by the Office of the Superintendent of Financial Institutions ("**regulated entity**") to consider Third-Party Risk Management Guideline B-10 ("**framework**") in the context of Google Cloud and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: section 2.2.2 (Due diligence), 2.2.3 (Concentration risk), 2.2.4 (Subcontracting risk), 2.3 (Risk management and mitigation), 2.4 (Monitoring and reporting), 4 (Technology and cyber risk in third-party arrangements), Annex I (Examples of due diligence consideration) and Annex II (Provisions for third-party arrangements). For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	**2.2.2) Due diligence** **Principle 4:** The FRFI should undertake due diligence prior to entering contracts or other forms of arrangement with a third party, and on an ongoing basis proportionate to the level of risk and criticality of the arrangement.		
2.	**2.2.2.1) A due diligence process is established** The FRFI should establish due diligence processes for third-party arrangements to apply initially and on an ongoing basis, including documented risk escalation, approval and acceptance processes.	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page.	N/A
3.	**2.2.2.2) Due diligence is performed proportionate to level of risk and criticality** The FRFI should conduct due diligence proportionate to the level of risk and criticality of each third-party arrangement:	See above.This is a customer consideration.	N/A
4.	• prior to entering into the arrangement;	See above.This is a customer consideration.	N/A
5.	• as part of the contract renewal process; and	See above.	N/A
6.	• periodically on an ongoing basis proportionate to the level of risk and criticality or whenever there are material changes to the third-party arrangement, such as the nature of the arrangement or its criticality.	See above.	N/A
7.	Due diligence should consider all relevant qualitative (i.e., operational) and quantitative (i.e., financial) factors related to the third-party arrangement. A non-exhaustive list of factors to consider in respect of high-risk and critical arrangements is set out in Annex 1 of this Guideline.	See Rows 86 to 105 for information on Annex 1.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
8.	**2.2.2.3) Out-of-Canada arrangements are considered** When considering third-party arrangements with a geographic presence outside of Canada (or subcontractors with a geographic presence outside of Canada) **the FRFI should review the legal requirements of relevant jurisdictions, as well as the political, legal, security, economic, environmental, social, and other risks that may impede the ability of the third party to provide services.**	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s) You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Transfers (Cloud Data Processing Addendum)
9.	**2.2.3) Concentration risk**		
10.	**2.2.3.1) Concentration risk is assessed** To determine the appropriate level of mitigation, the FRFI should assess concentration risk both prior to entering a contract or agreement and on an ongoing basis. Processes established should take reasonable steps to assess concentration risk over multiple dimensions including geography, supplier, and subcontractor. Throughout the process, concentration should be considered within the FRFI's business functions/units and legal entities, and across the FRFI's entire organization. To the greatest extent possible, FRFIs should also assess systemic concentration risk.	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
11.	**2.2.4) Subcontracting risk** **Principle 5**: The FRFI is responsible for identifying, monitoring and managing risk arising from subcontracting arrangements undertaken by its third parties.		
12.	**2.2.4.1) Risks introduced by subcontracting practices are identified and understood** The FRFI should assess risks arising from third-party subcontractors that could impact the FRFI.	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors
13.	Prior to entering a third-party arrangement the FRFI should identify and understand the third party's subcontracting practices, including:		
14.	• number and criticality of subcontractors;	See Row 12.	N/A
15.	• the adequacy and performance of the third party's own third-party risk management program, including assurance that significant performance, legal and regulatory requirements are aligned with the contract entered into with the FRFI; and	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors
16.	• impact of subcontracting arrangements on the FRFI's own concentration risk (refer to 2.2.3 above).	This is a customer consideration.	N/A
17.	**2.2.4.2) Monitor and manage subcontracting risks** The FRFI should ensure that they will receive appropriate ongoing updates and reporting on the third party's use of subcontractors so the FRFI can appropriately manage subcontracting risk. Depending on the level of risk and the criticality of services provided by the third party, the FRFI can achieve this by contractual provisions:		

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
18.	• prohibiting the use of subcontractors for certain functions;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never subcontract. Given the one-to-many nature of our service, if we agreed with one customer that we would not subcontract, we would potentially be denying all our customers the benefit motivating the subcontracting arrangement. To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice.	Subcontracting; Google Subcontractors
19.	• requiring that the FRFI be informed, in writing and on a timely basis, when a subcontractor is retained, or substituted, to carry out some of the functions contracted for the third party to perform;	You need enough time from being informed of a subcontractor change to perform a meaningful risk assessment before the change comes into effect. To ensure you have the time you need, Google provides advance notice before we engage a new subcontractor or change the function of an existing subcontractor.	Google Subcontractors
20.	• reserving a right of the FRFI to refuse a subcontractor; and	Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors
21.	• allowing the FRFI to commission or conduct an audit of subcontractors.	Google recognizes that subcontracting must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	Google Subcontractors
22.	**2.3) Risk management and mitigation** **Outcome:** Risks posed by third parties are managed and mitigated within the FRFI's Risk Appetite Framework.		
23.	**2.3.1). Written agreements / contracting** **Principle 6:** The FRFI should enter into written arrangements that set out the rights and responsibilities of each party.		

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
24.	**2.3.1.1) Clear responsibilities are set out in the agreement** OSFI expects third-party arrangements to be supported by a written contract or other agreement (e.g., service level agreement) that sets out the rights and responsibilities of each party and which has been reviewed by the FRFI's legal counsel. OSFI recognizes that there are certain third-party arrangements for which a customized contract may not be feasible, or for which a formal contract or agreement may not exist. Please see Section 3 of this Guideline for OSFI expectations related to such third-party arrangements.	The rights and responsibilities of the parties are set out in the Google Cloud Financial Services Contract	N/A
25.	**2.3.1.2) The third party is expected to comply with FRFI's provisions** To manage the risks associated with each third-party arrangement, the FRFI should structure its written agreement with the third party in a manner that allows it to meet the expectations set out in this Guideline. OSFI expects the FRFI to include in written agreements for high-risk and critical arrangements the provisions that are set out in Annex 2 of this Guideline.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation. Refer to Rows 106 to 126 for information on Annex 2.	Enabling Customer Compliance
26.	**2.3.2) Data security and controls (including data location)** **Principle 7:** Throughout the duration of the third-party arrangement, the FRFI and third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data.		
27.	**2.3.2.1) Responsibilities for security of records and data are established** Third-party agreements are expected to set out each party's responsibilities for the confidentiality, availability and integrity of records and data. Agreements should establish, among other things:		
28.	• the scope of the records and data to be protected;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account.	Enabling Customer Compliance.

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
29.	• availability of the records and timely access to data by the FRFI and OSFI, upon request;	You may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Regulator Information, Audit and Access
30.	• controls and monitoring over the third party's use of the FRFI's systems and information;	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google makes security resources, features, functionality and controls available that customers may use to secure and control access to customer data, including the Cloud Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls. • Cloud Identity and Access Management helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud resources. • Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. • Multi-Factor Authentication provides a wide variety of verification methods to help protect your user accounts and data. • The "Managing Google's Access to your Data" section of our Trusting your data with Google Cloud whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). • Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	Data Security; Additional Security Controls (Cloud Data Processing Addendum) Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
31.	• clear responsibilities of each party in managing data security;	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The security / confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you:	Confidentiality Data Security; Google's Security Measures (Data Processing Amendment)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. • Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
32.	• which party is liable for any losses that might result from a security breach; and	Refer to your Google Cloud Financial Services Contract.	Liability
33.	• notification requirements if there is a breach of security.	Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
34.	As appropriate, these agreements should also specify that the FRFI's data and records be isolated from those of other clients at all times, including during the transfer process and under adverse conditions (e.g., disruption of services). Based on the level of risk, data and records should be subject to the equivalent standard of protection at the third party that they would be at the FRFI.	To keep data private and secure, Google logically isolates each customer's data from that of other customers.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
35.	**2.3.2.2) Record keeping requirements** *The Bank Act, Insurance Companies Act*, and the *Trust and Loan Companies Act* (collectively, the FRFI Statutes), contain requirements with respect to certain records that FRFIs must prepare and maintain (the Records) OSFI expects the Records to be updated and accurate as at the end of each business day (Records that change less frequently than daily remain accurate until they change), and that the Records will be sufficiently detailed to enable:	Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. Google has multiple data centers in Canada. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. You may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Regulator Information, Audit and Access
36.	• OSFI to conduct an examination and inquiry into the business and affairs of the FRFI;	See above.	N/A
37.	• OSFI to manage the FRFI's assets, prior to the appointment of a liquidator, should the Superintendent take control of the FRFI's assets; and	See above.	N/A
38.	• The liquidator to conduct an effective liquidation of the FRFI's assets.	See above.	N/A
39.	Electronic Records must be capable of being reproduced in intelligible written form within a reasonable period of time. OSFI expects electronic Records to be accessible and intelligible without incurring additional costs and by using readily available commercial applications. For certain types of information, such as reinsurance arrangements or files on more complex activities, reproduced electronic records may not be sufficient for OSFI's review and the executed copy may need to be available, upon OSFI's request.	See above.	N/A
40.	The FRFI Statutes require FRFIs to keep copies of the Records at its head office, or at such other place in Canada as the directors of the FRFI think fit. If the Records are in electronic form, complete copies must be kept on a computer server(s) physically located at the places stipulated in the FRFI Statutes.	See above.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
41.	Certain FRFIs are exempted from the requirement to keep copies of the Records at the above noted places in Canada. In those circumstances, the FRFI must provide OSFI with immediate, direct, complete and ongoing access to the Records that are stored outside Canada.	See above.	N/A
42.	**2.3.3) Information rights and audit** **Principle 8:** The FRFI's third-party arrangements should allow the FRFI timely access to accurate and comprehensive information to assist it in overseeing third-party performance and risks. The FRFI should also have the right to conduct or commission an independent audit of a third party.		
43.	**2.3.3.1) The third party provides the FRFI with information and reporting** The third-party agreement should specify the type and frequency of information to be reported to the FRFI by the third party. This should include reports that allow the FRFI to assess whether performance measures are being met and any other information required for the FRFI's monitoring program, including risk measures (see Section 2.4).	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The Service Health Dashboard provides status information on the Services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring
44.	**2.3.3.2) The third party reports events that could materially impact the FRFI** The agreement should include requirements and procedures for the third party to report events in a timely manner to the FRFI that may materially affect the risks and delivery of the service.	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. You can also use Personalized Service Health to receive granular alerts about Google Cloud service disruptions, as a stop in your incident response, or integrated with your incident response or monitoring tools.	Significant Developments Data Incidents (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	
45.	**2.3.3.3) Service performance and controls are evaluated, and audit rights established, as appropriate** The agreement should give the FRFI and OSFI the right to evaluate the risk management practices related to the service provided. Specifically, the FRFI and OSFI should be able to evaluate the risks arising from the arrangement or appoint independent auditors to evaluate the risk management practices related to service provided and the risks arising from the relationship on the FRFI's or on OSFI's behalf. The FRFI and OSFI should also be able to access audit reports in respect of the service being performed for the FRFI.	Audit rights Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. Audit reports Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • -ISO/IEC 27001:2013 (Information Security Management Systems) • -ISO/IEC 27017:2015 (Cloud Security) • -ISO/IEC 27018:2014 (Cloud Privacy) • -PCI DSS • -SOC 1 • -SOC 2 • -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Regulator Information, Audit and Access
46.	The FRFI should employ a range of audit and information gathering methods (e.g., independent reports provided by third parties, individually performed or pooled audits).	Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.	N/A
47.	**2.3.4) Business continuity planning and testing** **Principle 9:** The FRFI's agreement with the third party should encompass the ability to deliver operations through disruption, including the maintenance, testing, and activation		

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	of business continuity and disaster recovery plans. The FRFI should have contingency plans for its critical third-party arrangements.		
48.	**2.3.4.1) Business continuity and recovery capabilities are established and tested** Third-party agreements should require the third party, at minimum, to:		
49.	• outline the third party's measures for ensuring continuity of services in the event of disruption;	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
50.	• test regularly the third party's business continuity and disaster recovery programs as they pertain to services provided to the FRFI;	See above.	N/A
51.	• notify the FRFI of test results; and	See above	N/A
52.	• address any material deficiencies.	See above	N/A
53.	Among other things, the FRFI's business continuity and disaster recovery plans should:		
54.	• address severe but plausible situations (either temporary or permanent), including prolonged disruptions and multiple simultaneous disruptions, where the third party could fail to continue providing service;	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications.	
55.	• document backup systems and redundancy capabilities that are commensurate with the criticality of the service provided; and	Regulated entities can use Google Cloud Back Up and Disaster Recovery to manage backups. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup.	N/A
56.	• ensure the FRFI has in its possession, or can readily access, all necessary records to allow the FRFI to sustain business operations, meet statutory obligations, and provide all information as may be required by OSFI, in the event of disruption to third-party services.	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. You also decide what data you provide to the services under your account and may access your data on the services at any time. Regulated entities may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Enabling Customer Compliance.
57.	As applicable, joint design and testing of business continuity plans and disaster recovery plans should be considered between the third party and the FRFI, commensurate with the criticality of the service.	In addition to testing our own environments, Google also provides a number of tools and resources that enable regulated entities to independently test their Google Cloud deployments. Our Disaster Recovery Scenarios for Data and Disaster Recovery for Applications articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively. You can also implement the following to help with your own testing: • **Automate infrastructure provisioning with Deployment Manager**. You can use Deployment Manager to automate the provisioning of VM instances and other Google Cloud infrastructure. If you're running your production environment on premises, make sure that you have a monitoring process that can start the disaster recovery process when it detects a failure and can trigger the appropriate recovery actions. • **Monitor and debug your tests with Cloud Logging and Cloud Monitoring.** Google Cloud has excellent logging and monitoring tools that you can access through API calls, allowing you to automate the deployment of recovery scenarios by reacting to metrics. When you're designing tests, make sure that you have appropriate monitoring and alerting in place that can trigger appropriate recovery actions.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
58.	**2.3.5) Contingency and exit strategy / planning**		
59.	**2.3.5.1) Contingency and exit strategies are developed to ensure continuity of critical services** The FRFI should establish contingency and exit plans proportionate to the level of risk and criticality of individual third-party arrangements to ensure continuity of the FRFI's operations through normal and stressed times. FRFIs should include the following elements in their documented plans for arrangements deemed high-risk or critical, and consider including them in their plans for arrangements deemed to have lower risk or criticality:	Google recognizes that, whatever the level of technical resilience that can be achieved on Google Cloud, regulated entities must plan for the scenario in which Google can no longer provide the service. We support such exit plans through: • Commitment to Open Source: many of our products and services are available in Open Source versions, meaning that they can be run on other Cloud providers or on-premise. • Commitment to common standards: our platform supports common standards for hosting applications in virtual machines or containers, which can be replicated by alternative services on other Cloud providers or on-premise. • Anthos multi-Cloud management: our multi-Cloud management product, Anthos, allows customers to run and manage an increasing range of services in the same way as on Google Cloud across other Cloud providers or on-premise. Refer to our Planning for the Worst paper for more information about how Google Cloud supports Reliability, Resilience, Exit and Stressed Exit. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on our commitment to open source and common standards.	N/A
60.	• triggers for invoking exit/contingency plans;	See above.	N/A
61.	• activities to perform to maintain critical operations during disruptions or when exiting because of unplanned circumstances, such as failure or insolvency of the service provider (a "playbook" for stressed exit);	See above.	N/A
62.	• activities to perform when exiting through a planned and managed exit due to commercial, performance, or strategic reasons (a "playbook" for non-stressed exit);	See above.	N/A
63.	• reference to contractual provisions that could impact exit, such as notification requirements and provisions obliging the third party to provide services over a prescribed period of time following notification of termination;	Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help regulated entities achieve this, upon request, Google will	Transition Term

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		continue to provide the Services for 12 months beyond the expiry or termination of the contract.	
64.	• sufficient detail (e.g., alternative options or providers, supported by timelines, costs, resourcing, revenue impacts, and interim workarounds) so as to allow rapid execution; and	Refer to Row 59.	N/A
65.	• documented plans for responding to severe but plausible scenarios, including prolonged and multiple disruptions.	Refer to Row 59.	N/A
66.	Contingency plans and exit strategies should be reviewed regularly, and more frequently in the event of material changes to the third-party arrangements.	This is a customer consideration.	N/A
67.	**2.4) Monitoring and reporting** **Outcome:** Third-party performance is monitored and assessed, and risks and incidents are proactively addressed.		
68.	**Principle 10:** The FRFI should monitor its third-party arrangements to verify the third party's ability to continue to meet its obligations and effectively manage risks.		
69.	**2.4.1) Oversight of third-party provider**		
70.	**2.4.1.1) The FRFI monitors its third-party arrangement(s)** The FRFI should monitor its third-party arrangement(s) to ensure that the service is being delivered in accordance with the terms of the agreement, and that the third party remains financially sound.	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: • The Service Health Dashboard provides status information on the Services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Ongoing Performance Monitoring

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
71.	Monitoring should also cover regular oversight of current and emerging risks and risk acceptances and compliance of the third-party arrangement with the FRFI's risk policies and procedures and OSFI's expectations. Monitoring should be conducted at the individual arrangement level, as well as at an aggregate business unit, segment, platform, and enterprise level. The extent and frequency of monitoring should be proportionate to the level of risk and criticality of the third-party arrangement.	See above.	N/A
72.	**2.4.1.2) Metrics confirm residual risk remains within risk appetite** The FRFI should establish processes to confirm regularly that the residual risk of their third-party arrangements, individually and in aggregate, remains within the FRFI's risk appetite. To facilitate this outcome, the FRFI should establish and report metrics and associated thresholds to alert Senior Management when a threshold is being approached as well as triggers for invoking the FRFI's escalation process.	This is a customer consideration.	N/A
73.	**2.4.2) Incident management and reporting** **Principle 11:** Both the FRFI and its third-party should have documented processes in place to effectively identify, investigate, escalate, track, and remediate incidents to maintain risk levels within the FRFI's risk appetite.		
74.	**2.4.2.1) The third-party has clearly defined incident management processes** As part of an effective third-party risk management program, the FRFI should ensure that its third parties have clearly defined and documented processes for identifying, investigating, escalating, remediating and notifying the FRFI in a timely manner of incidents — including subcontractor incidents — that could directly or indirectly impact the third party's ability to deliver the contracted goods, business activities, functions and services.	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
75.	**2.4.2.2) Incident reporting and notification requirements of the third party support FRFI compliance with OSFI's incident reporting requirements** The FRFI should ensure that its written agreements with third parties contain adequate provisions to enable the FRFI to comply with its reporting requirements under OSFI's Technology and Cyber Security Incident Reporting Advisory (PDF). Such provisions could	See above. To assist customers with their own incident response, Google's notification will describe: • the nature of the Data Incident including the Customer resources impacted; • the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk;	Data Incidents (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	include, among other things, requirements to promptly notify the FRFI of technology and cybersecurity incidents (at the third party or the subcontractor) including providing information on each incident in line with the Advisory.	• the measures, if any, Google recommends that Customer take to address the Data Incident; and • details of a contact point where more information can be obtained. In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. Our Autonomic Security Operations (ASO) solution: • delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. • enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution. Information on Google's security products is available here. Here are some examples: • Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. • Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud environment. • Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud resources and changes to resources including VM instances, images, and operating systems.	
76.	**2.4.2.3) Internal incident management process is established** The FRFI should also have clearly defined internal processes for effectively managing and escalating third-party incidents and for subsequently tracking remediation. The processes established should clearly define accountabilities at all levels of the FRFI and triggers for escalation within the FRFI.	See above.	N/A
77.	**2.4.2.4) Incidents are investigated, analysed and results are shared** To ensure that remediation actions are sufficient, the FRFI should request that the third party perform root cause analysis and share the results for any incidents, commensurate with the severity/potential impact of the incident on the FRFI. The FRFI	At Google, we strive to learn from every incident and implement preventative measures to avoid future incidents. The actionable insights from incident analysis enable us to enhance our tools, trainings and processes, Google's overall security and privacy data	Data Incidents (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	should also perform its own root cause analysis, as appropriate. Remediation actions should be monitored by the FRFI.	protection program, security policies, and / or response efforts. The key learnings also facilitate prioritization of engineering efforts and building of better products. Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. During this process, the incident response team reviews the cause(s) of the incident and Google's response and identifies key areas for improvement. Refer to our Data incident response whitepaper for more information.	
78.	**4) Technology and cyber risk in third-party arrangements** **Outcome:** Technology and cyber operations carried out by third parties are transparent, reliable and secure.		
79.	OSFI recognizes that technology and cyber risks in third-party arrangements present elevated vulnerabilities to the FRFI. In addition to the expectations articulated earlier in this guideline, the FRFI should consider additional controls to manage technology and cyber risks stemming from its third-party arrangements.	Google publishes a number of resources to help customers understand how to configure robust security for our services: • Security best practices • Security use cases • Security blueprints	N/A
80.	**4.1) Clear roles and responsibilities are established for technology and cyber controls** As set out earlier in this guideline, and emphasized in Annex 2, establishing clear roles and responsibilities between the FRFI and the third party is essential to managing risk, ensuring accountability, and limiting ambiguity between the parties. When setting responsibilities for technology and cyber controls, the FRFI should consider the risk and criticality of its arrangement. Where necessary, the FRFI should establish more granular descriptions of the roles, responsibilities, and procedures that apply to each party when managing the configuration of technology assets.	We recognize that as a cloud provider we maintain significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of our data centers. It is important for regulated entities to have a clear understanding of the allocation of responsibility in the cloud, and in particular the boundaries of responsibility between your organization and the cloud service provider. Responsibility in the cloud is assigned as follows: • Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks. • Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications. Refer to our Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibilities between Google and our customers.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
81.	**4.2) Third parties comply with the FRFI's technology and cyber standards** Where necessitated by risk and/or criticality, the FRFI should establish processes to ensure that third parties with elevated levels of technology and cyber risk comply with FRFI standards—or recognized industry standards—for mitigating risk, notably in the areas of access management, and data security and protection.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001:2013 (Information Security Management Systems) -ISO/IEC 27017:2015 (Cloud Security) -ISO/IEC 27018:2014 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
82.	**4.3) Cloud-specific requirements are established** The FRFI should develop cloud-specific requirements to ensure that cloud adoption occurs in a planned and strategic manner. These specific requirements should optimize interoperability while remaining consistent with the FRFI's stated risk appetite. They should also augment existing FRFI controls and standards, notably in the areas of data protection, key management, and container management.	Google recognizes that you need to plan and execute your migration carefully. Our Migration to Google Cloud guide helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. In addition, our Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. Once on Google Cloud, you can leverage Risk Manager to continuously evaluate risk. Our Board of Directors Handbook for Cloud Risk Governance provides practical guidance for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. In particular, it explains how adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk.	N/A
83.	These requirements should be accompanied by robust cloud governance to provide proper oversight and monitoring of compliance with the FRFI's risk management practices and alignment to the broader technology strategy.	Our Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment. In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind. Refer to our Board of Directors Handbook for Cloud Risk Governance whitepaper for more information, including about how control design and ownership evolves in the cloud.	
84.	**4.4) Cloud portability is considered** In addition to planning appropriate exit strategies (see Section 2.3.5), the FRFI should also consider portability when entering an arrangement with a cloud service provider and as part of the design and implementation process in cloud adoption. As part of the consideration, FRFI should assess benefits and risks of portability and mitigants in the absence of portability.	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud. In addition, Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page.	Data Export (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
85.	The FRFI should consider strategies (e.g., multi-cloud design) to build resilience and mitigate cloud service provider concentration risk (see Section 2.2.3).	See above.	N/A
86	**Annex 1 – Examples of due diligence consideration**		
87	Before entering an arrangement with a third party—whether written or not—and on an ongoing basis thereafter, the FRFI should perform due diligence proportionate to the risk and criticality of the third-party arrangement. In respect of its high-risk and critical arrangements at minimum, the FRFI should perform due diligence that consists of the following non-exhaustive factors:	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below. In addition, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of security, privacy, business continuity, and operational resiliency controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page.	N/A
88	a. Experience, technical competence, and capacity of the third party to implement and support the activities it is being engaged to provide, including, where applicable, the experience, technical competence, and capacity of subcontractors;	Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud's capabilities is available on our Choosing Google Cloud page. Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. Information about our referenceable customers is available on our Google Cloud Customer page. In addition, our Financial Services Cloud Blog and Financial Services solutions page explains how financial services institutions can and are using Google Cloud to help drive business transformation to support data-driven innovation, customer expectations, and security & compliance. Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you.	N/A Google Subcontractors

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	
89	b. Financial strength of the third party to deliver successfully on the third-party arrangement;	You can review Google's corporate and financial information on Alphabet's Investor Relations page.	N/A
90	c. Compliance with applicable laws, rules, regulations and regulatory guidance within Canada and other relevant jurisdictions;	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. In addition, as part of your migration to the cloud, you may need to validate our compliance documentation, certifications, and controls. Google Cloud creates and shares mappings of our industry leading security, privacy, and compliance controls to standards from around the world. We also regularly undergo independent verification—achieving certifications, attestations, and audit reports to help demonstrate compliance. Refer to our Compliance Resource Center for more information.	Representations and Warranties
91	d. Reputation risk associated with the third-party relationship or its services, including existence of any recent or pending litigation, investigation or complaints against the third party;	Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page.	N/A
92	e. Strength of the third party's risk management programs, processes, and internal controls as well as the reporting environment (the FRFI should determine if there is alignment with the FRFI's risk management processes and controls);	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2	Certifications and Audit Reports

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	
93	f. The third party's capacity to:		
94	• manage technology and cyber risks in accordance with the expectations outlined in OSFI's Guideline B-13: Technology and Cyber Risk Management and	Infrastructure and security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The security and confidentiality of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud	Confidentiality Data Security; Google's Security Measures (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: • Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. • Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints	
95	• provide the FRFI with sufficient and timely information to comply with its reporting requirements under OSFI's Technology and Cyber Security Incident Reporting Advisory (PDF);	Google recognizes that to effectively manage your use of the Services you need sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.	Significant Developments

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
96	g. Strength of the third party's information security programs including their alignment with the FRFI's programs;	Google has a dedicated security team, which includes some of the world's foremost experts in information security, application security, cryptography, and network security. This team maintains our defense systems, develops security review processes, builds security infrastructure, and implements our security policies. The team actively scans for security threats using commercial and custom tools. The team also conducts penetration tests and performs quality assurance and security reviews. Members of the security team review security plans for our networks and services, and they provide project-specific consulting services to our product and engineering teams. The security team monitors for suspicious activity on our networks and addresses information security threats as needed. The team also performs routine security evaluations and audits, which can involve engaging outside experts to conduct regular security assessments. Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance, including: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Refer to our security whitepaper for more information.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
97	h. The third party's capacity to provide critical services through disruption by examining its business continuity and disaster recovery plans, including the quality of such plans and the frequency and results of testing;	Resilience Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. In addition, refer to our Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired reliability outcomes for your applications. Business Continuity Plan Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide.	Business Continuity and Disaster Recovery
98	i. The third party's reliance on, and capacity to, manage subcontractors;	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Google Subcontractors

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights).	
99	j. Impact of the third-party arrangement, including its subcontractors, on concentration risk;	Google recognizes the importance of continuity for regulated entities and for this reason we are committed to data portability and open-source. Refer to our Engaging in a dialogue on customer controls and open cloud solutions blog post and our Open Cloud page for more information on how Google's approach to open source can help you address vendor lock-in and concentration risk. To manage concentration risk, you can choose to use Anthos to build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. For more information, refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud.	Data Export (Cloud Data Processing Addendum)
100	k. Geographic location of the third party's operations and that of its subcontractors;	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. • Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. • Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s)	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Transfers (Cloud Data Processing Addendum)
101	l. Ability and ease of substituting the third party with another third party and impact of such substitution on the FRFI's operations;	Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	Data Export (Cloud Data Processing Addendum)
102	m. Portability of applications/services provided by a third party to another third party or the FRFI;	Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here.	Data Export (Cloud Data Processing Addendum)
103	n. Third party's insurance coverage;	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
104	o. Third party's values and business objectives, code of conduct and related policies, culture, and their alignment with those of the FRFI; and	You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct, which addresses conflicts of interest.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
105	p. Political or legal risks related to the jurisdiction of the third party, or the jurisdictions of subcontractors.	Refer to Row 100.	N/A
106	**Annex 2 – Provisions for third-party agreements**		
1072 2	This annex provides a non-exhaustive list of provisions that FRFIs should include in high-risk and critical third-party agreements. Consideration should be given to adding these provisions to agreements with other third parties as appropriate, proportionate to the risk and criticality posed by the third party.		
108	a. **Nature and scope of the arrangement**: The agreement should specify the nature and scope of the arrangement, including provisions that address the frequency, content and format of services, duration of the agreement, and physical location of the services being provided.	Scope The Google Cloud services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement. Location To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. ● Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. ● -Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: ● The same robust security measures apply to all Google facilities, regardless of country / region. ● Google makes the same commitments about all its subprocessors, regardless of country / region.	Services Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum)

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper.	Data Location (Service Specific Terms)
109	b. **Roles and responsibilities**: The agreement should clearly establish the roles and responsibilities of the FRFI and the third-party and subcontractors, including for managing technology and cyber risks and controls.	The roles and responsibilities of the parties are set out in the Google Cloud Financial Services Contract.	N/A
110	c. **Use of subcontractors**: The agreement should establish parameters on the use of subcontractors and require the third-party to notify the FRFI of any subcontracting of services. The FRFI should have the ability to conduct due diligence, in order to evaluate the impacts from the change in service.	Google recognizes that regulated entities need to consider the risks associated with subcontracting. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors; ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to the subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors
111	d. **Pricing**: The agreement should set out the basis for calculating fees relating to the services being provided.	Refer to your Google Cloud Financial Services contract. Prices and fee information are also publicly available on our SKUs page. Refer to our Pricing page for more information.	Payment Terms
112	e. **Performance measures**: The agreement should establish performance measures that allow each party to determine whether the commitments set out in the agreement are being fulfilled.	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page.	Services

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
113	f. **Ownership and access**: The agreement should identify and establish ownership of all assets (intellectual and physical) related to third-party arrangements, including assets generated or purchased pursuant to the arrangement. The agreement should also specify whether and how the third party has the right to use the FRFI's assets (e.g., data, hardware and software, system documentation or intellectual property), including authorized users, and the FRFI's right of access to those assets.	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. Google will not use your copyright, patent, trademark or logo without your prior approval.	Intellectual Property Protection of Customer Data Marketing and Publicity
114	g. **Security of records and data**: The agreements should govern the confidentiality, integrity, security, and availability of records and data.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Data Security; Google's Security Measures (Cloud Data Processing Addendum)
115	h. **Notifications to the FRFI**: The agreement should require the third party to notify the FRFI of:		
116	i. incidents/events (at the third party or a subcontractor) that impact or could impact services provided, the FRFI's customers/data or the FRFI's reputation;	Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard page.	Significant Developments
117	ii. technology and cyber security incidents (at the third party or a subcontractor) to enable the FRFI to comply with its reporting requirements under OSFI's Technology and Cyber Security Incident Reporting Advisory (PDF);	Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	Data Incidents (Cloud Data Processing Addendum)
118	iii. changes in ownership of the third party;	Google will provide advance notice to you if it experiences a relevant change in control.	Change of Control
119	iv. significant organizational/operational changes;	Information about our areas of investment and growth as well as risk factors is available in our annual reports on Alphabet's Investor Relations page.	N/A

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		.	
120	v. material non-compliance with regulatory requirements (i.e. regulatory enforcement) or litigation.	Information about material pending legal proceedings is available in our annual reports on Alphabet's Investor Relations page. .	N/A
121	i. **Dispute resolution**: The agreement should incorporate a protocol for resolving disputes. The agreement should also specify whether the third party must continue providing the service during a dispute and the resolution period, as well as the jurisdiction, governing law(s), and rules under which the dispute will be settled.	Refer to your Google Cloud Financial Services Contract.	Governing Law
122	j. **Regulatory compliance**: The agreement should enable the FRFI to comply with all applicable legislative and regulatory requirements, including, but not limited to, location of records and privacy of client information.	Google recognizes that regulated entities require assistance from Google to enable them to ensure compliance with applicable laws and regulations. We are committed to working with regulated entities in good faith to provide this assistance. In particular, we appreciate that you will need to have confidence that the Google Cloud Financial Services Contract continues to support your compliance requirements. We are committed to working with you throughout our relationship to address the impact of changes in law or regulation.	Enabling Customer Compliance
123	k. **Business continuity and recovery**: The agreement should require the third party to outline measures for ensuring continuity of services in the event of disruption including testing and reporting expectations and mitigation requirements, as well as requirements of the third party to monitor and manage technology and cyber security risk.	Continuity Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. Technology and cyber security risk Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open	Business Continuity and Disaster Recovery Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		source, and purpose-built in-house tools, and includes the following: quality assurance processes, software security reviews, intensive automated and manual penetration efforts (including extensive Red Team exercises) and external audits. The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution. To help improve detection capabilities, the vulnerability management organization focuses on high-quality indicators that separate noise from signals that indicate real threats. The organization also fosters interaction with the industry and with the open source community. Refer to our security whitepaper for more information. In addition: • Google publishes Threat Horizons intelligence reports to help keep your organization on top of the latest developments in the security landscape: https://cloud.google.com/security/gcat • Google publishes bulletins that contain public security updates, vulnerabilities and known issues for certain Google Cloud Services, via https://cloud.google.com/support/bulletins	(Security Measures) (Cloud Data Processing Addendum)
124	l. **Default and termination**: The agreement should specify what constitutes a default, or right to terminate, identify remedies, and allow for opportunities to cure defaults or terminate the agreement. Appropriate notice should be required for termination of the service and, where applicable, the FRFI's assets should be returned in a timely fashion. Any data and records should be returned to the FRFI in a format that allows the FRFI to sustain business operations without unreasonable expense. The agreement should not contain any terms that inhibit OSFI, or any other resolution authority or financial compensation scheme, from carrying out their	Termination Regulated entities can elect to terminate our contract for convenience with advance notice, including: • if necessary to comply with law; or • if directed by a supervisory authority. Regulated entities can terminate our contract with advance notice: • for Google's material breach after a cure period;	Term and Termination

OSFI - Third-Party Risk Management Guideline B-10 (April 2023)

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	mandate in times of stress or resolution. For example, the agreement should, among other things, remain valid and enforceable in resolution provided there is no default in payment obligations.	• for change of control; or • for Google's insolvency. Retrieval Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here. Resolution Google recognizes that regulated entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution.	Data Export (Cloud Data Processing Addendum) Support through Resolution
125	m. **Insurance**: The agreement should require the third party to obtain and maintain appropriate insurance and disclose the general terms and conditions of the insurance coverage. The agreement should also require the third party to notify the FRFI in the event of significant changes in insurance coverage.	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment.	Insurance
126	n. **Prudent risk management**: The agreement should include any additional provisions necessary for the FRFI to prudently manage its risks in compliance with this Guideline.	This is a customer consideration.	N/A